

PORTABLE TERMINAL AND PORTABLE TERMINAL INFORMATION PROTECTING METHOD

Patent Number: JP9215057
Publication date: 1997-08-15
Inventor(s): YAMAGUCHI MUNEAKI
Applicant(s): HITACHI LTD
Requested Patent: ☐ JP9215057
Application
Number: JP.19960016402.19960201
Priority Number(s):
IPC Classification: H04Q7/38; G06F1/00; G09C1/00; H04L9/32; H04M3/42;
H04M11/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide an information protection system and a portable terminal with which a terminal can be easily used at ordinary time and personal information left in the terminal can be protected and collected when the terminal is lost.

SOLUTION: According to a register request for information protection issued from a portable terminal 14, the security management data of the terminal 14 are registered in a security controller 10 connected to a radio network. When the terminal is lost and the owner of the portable terminal 14 requests the information protection to the security controller 10, an information protecting instruction is transmitted through the radio network to the portable terminal 14, and important information in the terminal is collected into the security controller 10 and made invalid by a dedicated program inside the portable terminal 14. Thus, even when the portable terminal 14 is lost, the important information can be collected and prevented from being abused.

Data supplied from the esp@cenet database - 12

JP Laid-open Publication No. Hei 9-215057 card

Portable Terminal and Portable Terminal Information Protecting
Method

[0041]

At step 291, processing to protect confidentiality of terminal information (either invalidation or rewriting) is applied (291). Protection of data confidentiality is achieved, for example, by means of erasure of terminal information in a memory or conversion of the information to false data.

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平9-215057

(43)公開日 平成9年(1997)8月15日

(51)Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 Q 7/38			H 0 4 B 7/26	1 0 9 R
G 0 6 F 1/00	3 7 0		G 0 6 F 1/00	3 7 0 E
G 0 9 C 1/00	6 6 0	7259-5 J	G 0 9 C 1/00	6 6 0 D
H 0 4 L 9/32			H 0 4 M 3/42	Z
H 0 4 M 3/42			11/00	3 0 2
審査請求 未請求 請求項の数28 O L (全 23 頁) 最終頁に続く				

(21)出願番号 特願平8-16402

(22)出願日 平成8年(1996)2月1日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 山口 宗明

東京都国分寺市東恋ヶ窪1丁目280番地

株式会社日立製作所中央研究所内

(74)代理人 弁理士 小川 勝男

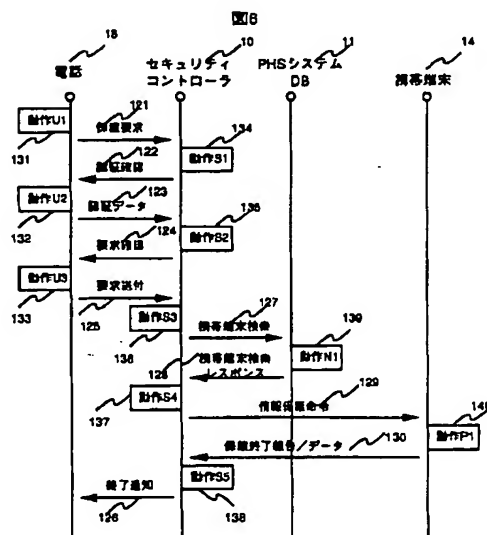
(54)【発明の名称】 携帯端末および携帯端末情報保護方法

(57)【要約】

【課題】通常時の端末使用を容易にし、端末紛失時に端末内に残された個人情報の保護、回収を可能にした情報保護システムおよび携帯端末の提供。

【解決手段】携帯端末14から発行した情報保護のための登録要求に従って、無線ネットワークに接続されたセキュリティコントローラ10に、上記端末のセキュリティ管理データを登録しておく。端末紛失時に、携帯端末の所有者がセキュリティコントローラに情報保護を要求すると、無線ネットワークを通じて、当該携帯端末に情報保護命令が送信され、携帯端末内にある専用プログラムによって、端末内重要情報のセキュリティコントローラへの回収と無効化が行われる。

【効果】携帯端末が紛失しても重要情報を回収し、悪用を阻止できる。



【特許請求の範囲】

【請求項1】無線通信手段と、出力手段と、入力手段と、ユーザデータを蓄積するためのメモリ手段と、上記入力手段からのユーザ操作入力に応じて、上記メモリ手段へのユーザデータの書き込み、読み出し、上記出力手段への情報の出力、および上記無線通信手段を介して他装置との情報の交信を行うためのデータ処理手段とからなる携帯端末装置において、

上記メモリ手段に記憶されているデータについての情報保護要求者を認証するための認証情報を記憶する手段と、

上記無線通信手段によって受信された情報保護命令メッセージに含まれる認証情報と上記記憶手段に予め記憶してある認証情報との対応関係から情報保護要求の正当性をチェックし、正当性が確認された場合に、上記メモリ手段に蓄積されている特定のユーザデータを無効化するための所定のデータ処理手順を記述した情報保護用ソフトウェアとを備え、

上記データ処理手段が、上記無線通信手段からの通知にตอบสนองして上記情報保護用ソフトウェアを実行し、上記特定のユーザデータを無効化して他人による利用を阻止するようにしたことを特徴とする携帯端末装置。

【請求項2】前記メモリ手段が、一般情報領域と保護情報領域とからなり、

前記データ処理手段が、上記情報保護用ソフトウェアを実行することにより、上記保護情報領域に蓄積されているユーザデータを無効化することを特徴とする請求項1に記載の携帯端末装置。

【請求項3】前記情報保護用ソフトウェアが、前記メモリ手段内に蓄積されている保護対象とすべきユーザデータのファイル識別情報を予め保持しており、

前記データ処理手段が、上記情報保護用ソフトウェアを実行することにより、上記ファイル識別情報で特定されたユーザデータを無効化することを特徴とする請求項1に記載の携帯端末装置。

【請求項4】前記情報保護用ソフトウェアが、ユーザデータ無効化に先立って、該当ユーザデータを前記情報保護命令メッセージの送信元に送信するための手順を含み、

前記データ処理手段が、上記情報保護用ソフトウェアを実行することにより、特定のユーザデータを他装置に回収した後、無効化することを特徴とする請求項1～請求項3の何れかに記載の携帯端末装置。

【請求項5】前記情報保護用ソフトウェアが、前記情報保護命令メッセージに含まれる処理区分コードに応じて、ユーザデータを無効化する前に、該ユーザデータを上記情報保護命令メッセージの送信元装置に選択的に送信するための手順を含み、

前記データ処理手段が、上記情報保護用ソフトウェアを実行することにより、上記ユーザデータを他装置に選択

的に回収動作した後、無効化することを特徴とする請求項1～請求項3の何れかに記載の携帯端末装置。

【請求項6】前記情報保護用ソフトウェアが、データ消去によって前記ユーザデータを無効化させることを特徴とする請求項4または請求項5に記載の携帯端末装置。

【請求項7】前記情報保護用ソフトウェアが、データ変換によって前記ユーザデータを無効化させることを特徴とする請求項4または請求項5に記載の携帯端末装置。

【請求項8】前記情報保護要求メッセージの受信時に前記無線通信手段から出力される割込み信号にตอบสนองして、前記データ処理手段および前記メモリ手段の電源を自動的に投入動作する電源制御手段を備えたことを特徴とする請求項1～請求項7の何れかに記載の携帯端末装置。

【請求項9】携帯端末が保持しているユーザ情報の保護に必要なセキュリティ管理データをセキュリティ制御装置に登録するステップと、

携帯端末の所有者が、上記セキュリティ制御装置に対して、紛失状態にある携帯端末について情報保護を要求するステップと、

上記情報保護要求を受けたセキュリティ制御装置が、予め登録してあるセキュリティ管理データに基づいて情報保護命令メッセージを生成し、無線ネットワークを介して上記紛失状態にある携帯端末宛に送信するステップと、

上記情報保護メッセージを受信した携帯端末が、該端末内に保持する所定のユーザ情報について、他人による利用を阻止するためのデータ処理を施すステップとからなることを特徴とする携帯端末情報保護方法。

【請求項10】前記セキュリティ制御装置が、上記情報保護を要求された携帯端末について無線ネットワークによる通信が可能な状態にあるか否かをチェックし、通信可能な状態にあることを確認して、前記情報保護命令メッセージを送信することを特徴とする請求項9に記載の携帯端末情報保護方法。

【請求項11】前記セキュリティ制御装置が、上記情報保護を要求された携帯端末について無線ネットワークによる通信が可能な状態にあるか否かをチェックし、通信不能な状態にあった場合、上記携帯端末との無線通信可否を所定の繰り返しパターンで繰り返すことを特徴とする請求項10に記載の携帯端末情報保護方法。

【請求項12】前記セキュリティ制御装置が、無線ネットワークに接続された移動端末データ管理装置に対して、前記情報保護を要求された携帯端末の状態を問合せ、

上記問合せを受けた移動端末データ管理装置が、上記携帯端末の位置登録の有無を上記セキュリティ制御装置に通知し、もし、現在位置が未登録状態にあった場合には、上記携帯端末について状態問合せを受けたことを記憶しておき、該当携帯端末が位置登録された時点で上記セキュリティ制御装置に通知し、

上記セキュリティ管理装置が、上記移動端末データ管理装置からの通知に応じて、前記情報保護命令メッセージを送信するようにしたことを特徴とする請求項9に記載の携帯端末情報保護方法。

【請求項13】前記セキュリティ制御装置に登録されるセキュリティ管理データが、携帯端末のアドレス情報と、登録者識別情報と、登録者認証情報とを含み、前記情報保護の要求時に、要求者が自分の識別情報と認証情報を提示し、上記セキュリティ制御装置が、上記提示された情報とセキュリティ管理データとして既に登録済の情報とに基づいて上記要求者の正当性をチェックし、正当性が確認された場合に、前記情報保護命令メッセージの生成と送信を行うことを特徴とする請求項9～請求項12の何れかに記載の携帯端末情報保護方法。

【請求項14】前記セキュリティ制御装置から送信される情報保護命令メッセージが前記認証情報を含み、上記情報保護命令メッセージを受信した携帯端末が、該受信メッセージから抽出した認証情報と該携帯端末内に予め設定されている認証情報とに基づいて、上記受信メッセージの正当性をチェックし、正当性が確認された場合に、前記所定のユーザ情報について他人の利用を阻止するためのデータ処理を実行することを特徴とする請求項13に記載の携帯端末情報保護方法。

【請求項15】前記情報保護命令メッセージを受信した携帯端末が、予め指定してある所定のメモリ領域のユーザ情報について、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項9～請求項14の何れかに記載の携帯端末情報保護方法。

【請求項16】前記セキュリティ制御装置に登録されるセキュリティ管理データが、保護対象となる情報を特定するためのファイル識別情報を含み、前記セキュリティ制御装置が、前記情報保護命令メッセージ中に上記ファイル識別情報を設定し、上記情報保護メッセージを受信した携帯端末が、受信メッセージ中のファイル識別情報で特定されたユーザ情報について、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項9～請求項14の何れかに記載の携帯端末情報保護方法。

【請求項17】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報を上記セキュリティ制御装置に送信した後、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項9～請求項16の何れかに記載の携帯端末情報保護方法。

【請求項18】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報を上記メッセージ中で指定された暗号鍵によって暗号化した形で上記セキュリティ制御装置に送信することを特徴とする請求項17に記載の携帯端末情報保護方法。

【請求項19】前記情報保護命令メッセージを受信した

携帯端末が、保護対象となった前記所定のユーザ情報を消去することによって、他人の利用を阻止することを特徴とする請求項9～請求項18の何れかに記載の携帯端末情報保護方法。

【請求項20】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報にデータ変換を施すことによって、他人の利用を阻止することを特徴とする請求項9～請求項18の何れかに記載の携帯端末情報保護方法。

10 【請求項21】前記セキュリティ管理データの前記セキュリティ制御装置への登録が、保護対象となる携帯端末から無線ネットワークを介して行われることを特徴とする請求項9～請求項20の何れかに記載の携帯端末情報保護方法。

【請求項22】前記セキュリティ制御装置への情報保護要求が、電話を利用して行われることを特徴とする請求項9～請求項21の何れかに記載の携帯端末情報保護方法。

20 【請求項23】携帯端末と、無線ネットワークと、上記無線ネットワークに接続されたセキュリティ制御装置とからなり、

上記セキュリティ制御装置が、携帯端末に関するセキュリティ管理データを記憶するための記憶手段と、紛失状態にある携帯端末の所有者からのデータ保護要求に応じて、上記セキュリティ管理データに基づいてデータ保護命令メッセージを生成し、これを上記無線ネットワークを介して該携帯端末に送信するためのメッセージ生成送信手段を備え、

30 上記セキュリティ制御装置にセキュリティ管理データを登録済の携帯端末が、上記無線ネットワークと通信するための無線通信手段と、データ処理手段と、上記無線通信手段で受信したデータ保護命令メッセージにตอบสนองして上記データ処理手段によって実行すべき専用ソフトウェアとを備え、上記専用ソフトウェアの実行によって、上記携帯端末内の特定のデータを無効化するようにしたことを特徴とする携帯端末の情報保護システム。

【請求項24】前記セキュリティ制御装置が、前記携帯端末所有者からのデータ保護要求時に、上記所有者が提示した個人認証情報と前記セキュリティ管理データとして予め登録されている個人認証情報とに基づいて上記保護要求の受け付け可否を判定する判定手段を備え、受付可と判断されたデータ保護要求について前記データ保護命令メッセージの生成と送信を行うことを特徴とする請求項23に記載の携帯端末の情報保護システム。

【請求項25】前記セキュリティ制御装置のメッセージ生成送信手段が、前記データ保護命令メッセージ中に前記セキュリティ管理データで予め登録されている個人認証情報を含めた形でメッセージを送信し、前記携帯端末が、受信したデータ保護命令メッセージに含まれる個人認証情報と予め該携帯端末に記憶されてい

る個人認証情報とに基づいて、上記データ保護命令メッセージへの応答可否を判定する判定手段を備え、上記判定手段で応答可と判断されたデータ保護命令メッセージに回答して、前記特定のデータについてのデータ処理を実行するようにしたことを特徴とする請求項23または請求項24に記載の携帯端末の情報保護システム。

【請求項26】前記携帯端末の無線通信手段が、前記データ保護命令メッセージを識別し、前記データ処理手段の電源を自動的に投入するための電源制御手段を備えることを特徴とする請求項23～請求項25の何れかに記載の携帯端末の情報保護システム。

【請求項27】前記携帯端末の専用ソフトウェアが、前記特定のデータについて、前記セキュリティ制御装置に転送した後、データ消去またはデータ暗号化によって他人に対するデータ無効化を行うことを特徴とする請求項23～請求項26の何れかに記載の携帯端末の情報保護システム。

【請求項28】前記携帯端末が、前記セキュリティ制御装置への転送データを暗号化するための手段を備えることを特徴とする請求項27に記載の携帯端末の情報保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯端末および携帯端末情報保護方法に関し、更に詳しくは、マイクロプロセッサとメモリ手段と無線通信手段とを備えた可搬型端末、およびメモリに蓄積されたユーザ情報の保護方法に関するものである。

【0002】

【従来の技術】半導体メモリやマイクロプロセッサ等の電子技術の向上によって、ノート型のパーソナルコンピュータの他に、電子手帳、パーソナルデジタルアシスタント（Personal Digital Assistants：PDA）、新携帯情報ツールなどと呼ばれる携帯端末装置が実用化されている。特に小型化、軽量化された携帯端末装置は、上着のポケットなどに入れて容易に持ち運ぶことができ、移動途中でデータの入出力操作をしたり、通信機能を利用して出先からオフィス側の情報処理システムとデータ交信する等、利用形態も多様化している。

【0003】然るに、これらの携帯端末装置は、所有者本人によってオフィス外に持ち出され、また、鞆やポケット等に入れ持ち運ばれるため、移動途中で盗難に遭遇したり、不注意による紛失、置き忘れ等、本人の意に反した形で他人の手に渡る機会が増え、端末装置内に記憶された情報が第三者に参照、悪用される危険性が高まってきた。従来、秘密性の高い情報を保護するための方法として、アクセスを制限すべき情報ファイルにはパスワードを対応付けておき、利用者がこの情報ファイルを参照しようすると、システム側からパスワードの入

力を促し、入力されたパスワードが予め登録されている正規のものと一致した場合にのみ、アクセスを許容する方法が知られている。

【0004】

【発明が解決しようとする課題】携帯端末は、主として個人の所有物として利用され、オフィス内に設置された固定端末のように不特定の複数の利用者が共用したり、他人に貸し借りすることを前提としたものではない。このため、携帯端末の所有者は、端末が自分の管理下にある間は、携帯端末内にあるユーザ情報の保護について意識することは稀である。また、携帯端末の所有者は、携帯端末の蓄積情報を自分の所有物として気軽に扱うことを望み、他人に見られてはならない情報であっても、平常時には、手続き的に面倒な上述したパスワード等による秘密保護策はとらず、必要な情報を随時、迅速にアクセスできる操作環境で端末を利用することが多い。携帯端末の所有者が、端末内の蓄積情報について他人による参照と利用を是非とも避けたいと意識するのは、自分の端末が紛失したことに気付いた時である。

【0005】本発明の目的は、端末を紛失した時、該端末内に残された所有者にとって重要な情報が第三者に悪用されるのを防止できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。本発明の他の目的は、端末を紛失した時、該端末内に残された所有者にとって重要なユーザ情報を所有者の手元に回収できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。本発明のさらに他の目的は、通常時において端末内の蓄積情報へのアクセスが容易であり、端末紛失時に該端末内に残された所有者にとって重要なユーザ情報を保護できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するため、本発明の携帯端末情報保護方法および保護システムでは、携帯端末に格納されているユーザ情報を保護するために必要なセキュリティ管理データを無線ネットワークに接続されたセキュリティ制御装置に予め登録しておき、携帯端末の紛失に気付いた端末所有者が、上記セキュリティ制御装置に対して自分の携帯端末についての情報保護を要求すると、セキュリティ制御装置が、予め登録してあるセキュリティ管理データに基づいて情報保護命令メッセージを生成し、これを無線ネットワークを介して携帯端末に送信し、上記情報保護メッセージを受信した携帯端末が、端末内に保持する所定のユーザ情報について他人の利用を阻止するためのデータ処理を施すようにしたことを特徴とする。

【0007】本発明の実施例によれば、上記セキュリティ制御装置が、目的の携帯端末が無線ネットワークによ

る通信が可能な状態にあるか否かをチェックし、通信可能な状態にあることを確認して上記情報保護命令メッセージを送信し、もし通信不能な状態であれば、通信可否の確認を所定の繰返しパターンで繰り返すようにしている。上記情報保護命令メッセージの送信に先立って、上記セキュリティ制御装置が、無線ネットワークにおける移動端末データを管理する管理装置に対して目的携帯端末の状態を問合せ、上記移動端末データ管理装置が、セキュリティ制御装置に上記携帯端末の位置登録の有無を通知し、もし、位置登録されていなかった場合には、上記携帯端末について状態問合せを受けたことを記憶しておき、当該携帯端末が位置登録された時点で上記セキュリティ制御装置に通知するようにし、上記セキュリティ管理装置が、移動端末データ管理装置からの通知に応じて情報保護命令メッセージを送信するようにしてもよい。

【0008】本発明において、上記セキュリティ管理データは、例えば、携帯端末のアドレス情報（無線ネットワークにおけるアドレスまたは電話番号）と、登録者識別情報と、登録者認証情報とを含む。このような管理データを予めセキュリティ制御装置に登録しておくことによって、情報保護の要求時に、要求者（紛失した携帯端末の所有者）に自分の識別情報と認証情報を提示させ、セキュリティ制御装置が、上記提示された情報と、セキュリティ管理データとして既に登録済の情報とを照合して要求者の正当性をチェックし、正当性が確認された場合に限り、上記情報保護命令メッセージの生成と送信を行わせるようにすることができる。また、携帯端末に送信する情報保護命令メッセージに上記認証情報を設定しておき、上記情報保護命令メッセージを受信した携帯端末に、受信メッセージから抽出した認証情報と携帯端末内に予め設定されている認証情報とに基づいて上記受信メッセージの正当性をチェックさせ、正当性が確認された場合に限り、情報保護のためのデータ処理を実行させることができる。

【0009】本発明による携帯端末は、無線通信手段と、出力手段と、入力手段と、ユーザデータを蓄積するためのメモリ手段と、上記入力手段からのユーザ操作入力に応じて、上記メモリ手段へのユーザデータの書込み、読み出し、上記出力手段への情報出力、および上記無線通信手段を介して他装置との情報の交信を行うためのデータ処理手段とからなる携帯端末装置において、上記メモリ手段に記憶されているデータについての情報保護要求者を認証するための認証情報を記憶する手段と、上記無線通信手段によって受信された情報保護命令メッセージに含まれる認証情報と上記記憶手段に予め記憶してある認証情報との対応関係から情報保護要求の正当性をチェックし、正当性が確認された場合に、上記メモリ手段に蓄積されている特定のユーザデータを無効化するための所定のデータ処理手順を記述した情報保護用ソフ

トウェアとを備え、上記データ処理手段が、上記無線通信手段からの通知にตอบสนองして上記情報保護用ソフトウェアを実行し、上記特定のユーザデータを無効化して他人による利用を阻止するようにしたことを特徴とする。

【0010】保護すべきユーザデータを特定するために、本発明の携帯端末では、例えば、メモリ手段を一般情報領域と保護情報領域とに分けておき、情報保護上記保護情報領域に蓄積されているユーザデータについて無効化する。この代わりに、情報保護用ソフトウェアが、保護対象とすべきユーザデータのファイル識別情報を予め保持し、上記ファイル識別情報で特定されたユーザデータを無効化するようにしてもよい。ユーザデータの保護形態として、上記情報保護用ソフトウェアにより、ユーザデータ無効化に先立って、ユーザデータを他の装置、例えば、上記情報保護要求メッセージの送信元に転送し、後で端末所有者の手元に回収できるようにしてもよい。この場合、上記ユーザデータを暗号化して転送するようにしてもよい。

【0011】

20 【発明の実施の形態】図1は、無線ネットワークを利用した本発明による携帯端末情報の保護方法を実現するためのシステム全体構成を示す。図において、1は、有線網5を介して相互接続された複数の無線基地局12（12A～12N）と移動端末制御データを格納したデータベースシステム11とからなる無線ネットワーク、10は上記無線ネットワークに接続されたセキュリティコントローラ（セキュリティサーバ）である。14（14A～14M）は上記無線ネットワークを利用する移動端末であり、通常の移動電話機の他に、本発明が対象とする携帯情報端末（以下、単に携帯端末という）もこれらの移動端末の一種となる。以下の実施例では、無線ネットワーク1としてPHS(Personal Handy-phoneSystem)を適用した場合について説明する。有線網5には、図示しない交換機システムを介して、固定端末18や他の公衆電話通信網が接続される。但し、上記無線ネットワーク1には、携帯端末とセキュリティコントローラとの間で計算機コマンドおよびデータを含むメッセージの通信を可能とする他の方式のものを適用してもかまわない。

30 【0012】上記データベースシステム（PHSシステムDB）11には、移動端末制御データとして、移動端末（PHS電話機およびPHS機能内蔵の携帯端末）の位置情報や認証情報などが管理され、本実施例では、セキュリティコントローラ10は上記データベースシステムと結合されている。セキュリティコントローラ10は、携帯端末14の所有者からのセキュリティ登録要求に応じて、携帯端末14の情報保護に必要なセキュリティ管理データを登録しておき、電話18等の通信装置を介してユーザから携帯端末情報の保護要求を受けたとき、予め登録されているセキュリティ管理データに基づいて、ユーザの認証、携帯端末の特定を行い、無線ネッ

トワークシステムを介して、後述する目的端末の現在位置情報の入手と情報の保護動作を行う。携帯端末14の位置情報は、PHSシステムDB11をアクセスすることにより得られ、情報保護は、携帯端末14に情報保護命令を送信し、携帯端末に内蔵されている情報保護プログラムを実行させることにより実現する。

【0013】図2は、携帯端末の所有者によるセキュリティコントローラ10への情報保護登録の手順を示す。携帯端末14で登録操作57を行うと、セキュリティコントローラ10と接続され、セキュリティコントローラ10に登録要求51が送信される。セキュリティコントローラ10は、上記登録要求51に応答して登録受付動作61を実行し、要求元の携帯端末14に登録情報要求52を送付する。携帯端末14は、上記登録情報要求に応じて、所有者に情報保護に必要な情報を入力させ、これを登録情報53としてセキュリティコントローラ10に送信する。セキュリティコントローラ10は、上記登録情報53を解析した後、登録情報確認要求54を携帯端末4に送信する。所有者が、登録内容に誤りのないことを確認すると、登録確認応答55が携帯端末14からセキュリティコントローラ10に送付される。セキュリティコントローラ10は、上記登録確認応答を受信すると、登録情報確認動作63を実行し、登録情報53を登録データテーブルに登録し、携帯端末14に登録OKレスポンス56を送信して登録処理を終了する。同様に、携帯端末側でも、上記登録OKレスポンス56を受信し、これをユーザが確認して登録処理を終了する。

【0014】図3は、携帯端末とセキュリティコントローラとの間で通信される携帯端末情報保護用のメッセージフォーマット70を示す。メッセージ70は、システムID71、動作ID72、データ量73、データ内容74、およびCRC（サイクリック・リダンダンシー・チェック）75の5つのフィールドからなる。システムID71には、このメッセージが携帯端末情報保護用のものであることを示すコードが設定される。動作ID72は、このメッセージの種類を示し、登録要求51、登録情報要求52等を識別するための識別子が設定される。データ量73は、後続するデータ内容フィールド74のデータ量をバイト単位で示し、CRC75は、動作IDフィールド72からデータ内容フィールド74までのデータ誤りチェックに利用される。

【0015】登録要求51に回答してセキュリティコントローラ10から携帯端末に送信される登録情報要求メッセージ52のデータ内容74は、データフォーマット76で示すように、必要データひな型79と暗号鍵A：80とを含む。必要データひな型79は、登録情報53として必要な情報項目を携帯端末所有者に表示するためのデータであり、入力すべき情報項目を表す文字列とそのバイト長とで構成されている。暗号鍵A：80は、例えば、公開暗号鍵方式における公開暗号鍵であり、携帯

端末14は、登録情報53を上記暗号鍵Aを用いて暗号化した形で、セキュリティコントローラに送信する。

【0016】登録情報メッセージ53のデータ内容74は、データフォーマット77で示すように、携帯端末識別ID81、携帯端末電話番号82、登録者ID83、認証情報84、処理番号85、および暗号鍵B：86を含む。携帯端末識別ID81は、携帯端末のシリアルナンバーであり、セキュリティコントローラが携帯端末と通信する際に、正しい携帯端末と通信しているか否かの判定に用いられる。携帯端末電話番号82は、携帯端末が内蔵するPHSの電話番号であり、セキュリティコントローラ10は、この電話番号によって、紛失状態にある携帯端末を呼び出す。登録者ID83は、携帯端末所有者のIDであり、セキュリティコントローラは、携帯端末情報保護サービスの実行に際して、このIDで利用者とセキュリティ管理データを特定する。認証情報84は、携帯端末情報保護サービスの要求者が登録者本人か否かを確認するための暗証情報（パスワード）である。処理番号85は、端末情報保護の形態を示す。例えば、端末が保持する情報（保護情報）を消去する場合は「処理番号＝1」、保護情報をセキュリティコントローラ側に回収（転送）した後、端末の保持する情報を消去する場合は「処理番号＝2」、の如く端末情報保護の形態（種類）をコード化しておき、端末所有者は、登録時に予め情報保護の形態を指定しておく。暗号鍵B：86は、公開暗号鍵方式の公開暗号鍵であり、セキュリティコントローラから携帯端末に送信する情報を暗号化するために用いられる。

【0017】登録OKレスポンス56のデータ内容74は、データフォーマット78で示すように、登録者ID83と処理番号85を含む。処理番号85は、上記登録情報メッセージ53において利用者が指定し、セキュリティコントローラ側で受け付けられた処理番号を示す。

【0018】図4は、登録手続きのために携帯端末に表示されるデータ入力画面の1例を示す。90は登録開始画面、91は登録情報入力画面、92は所有者確認画面であり、端末所有者は、表示内容に従って順次にデータを入力する。登録開始画面90において、メニュー93から「セキュリティ登録」を選択すると、登録ウィンドウ94が表示される。登録ウィンドウ94には、端末紛失時の情報保護を要求するとき使用する非常時連絡先電話番号と、情報登録処理の実行可否を指示するための

「YES（はい）」、「NO（いいえ）」のボタンが用意されている。情報登録処理を実行しようとする端末所有者は、上記非常時連絡先電話番号を手帳等にメモした後、「YES（はい）」ボタンを選択する。この操作によって、携帯端末からセキュリティコントローラ10へ自動的にダイヤルされ、コネクションが確立されると、携帯端末からセキュリティコントローラ10に登録要求51が送信される。なお、上記自動ダイヤルされる電話

番号は、上記非常時連絡先電話番号とは別のものとする。また、上記非常時連絡先電話番号は、携帯端末にロードされる情報保護用のソフトウェアの説明書で確認するようにしてもよい。

【0019】登録情報入力画面91は、登録情報要求メッセージ52でセキュリティコントローラ10から送信された必要データひな形79に基づいて構成される登録情報入力ウィンドウ95を有し、端末所有者は、このウィンドウで登録情報（セキュリティ管理データレコード）として必要な複数項目のデータを入力する。全てのデータ項目の入力を終え、所有者が送信ボタンを選択すると、データ内容74としてデータフォーマット77の内容をもつ登録情報メッセージ53が生成され、セキュリティコントローラ10に送付される。ユーザ確認画面92は、セキュリティコントローラ10から登録OKレスポンス56を受信した時、携帯端末に表示される画面であり、終了ボタンと登録情報を含むユーザ確認ウィンドウ96が表示される。所有者が、終了ボタンを選択すると登録処理が終了する。このとき、セキュリティ管理データの一部、例えば、登録者IDとパスワードは、携帯端末内の不揮発性メモリに記憶保持される。

【0020】図5は、登録処理時にセキュリティコントローラ10が実行する処理プログラムのフローチャートの1例を示す。ブロック61、62、63は、それぞれ図2に示した登録受付動作61、登録情報受付動作62、登録情報確認動作63に対応している。セキュリティコントローラ10は、携帯端末からの着信待ち状態（ステップ101）にあり、着信がなければ、常駐処理（102）によって待ち状態を繰り返す。メッセージが受信されると、メッセージデータ（入力データ）をチェック（103）し、受信メッセージが登録要求51か否かを判定する（104）。登録要求51であれば、登録情報要求データ52を作成し、携帯端末に送信（106）した後、次のメッセージの受信を待つ（107）。上記最初のメッセージが登録要求51でなければ、その他の処理105を行う。

【0021】次のメッセージとして暗号鍵Aで暗号化された登録情報53を受信すると、上記暗号鍵Aと対応する秘密暗号鍵を適用して登録情報をで読読、解析（108）した後、登録情報確認要求メッセージ54を作成して、携帯端末に送信（109）し、次のメッセージの受信を待つ（110）。上記登録情報確認要求メッセージ54のデータ内容74には、セキュリティコントローラ10が受信した登録情報メッセージ53のデータ内容77を含む。携帯端末からの登録確認応答55を受信すると、既に受信済の登録情報をセキュリティ管理データとして登録（113）し、登録OKレスポンスを作成して携帯端末に送信する（114）送付する。なお、携帯端末側から登録確認応答55として、登録情報メッセージ53と同様のデータ内容を持つメッセージを送信させ、

破線で示すように、受信登録確認応答メッセージ55のデータ内容を読読、解析した後、既に受信済の登録情報と比較し（112）、一致した場合に登録処理（113）し、不一致の場合は、登録情報要求ステップ（106）から再実行するようにしてもよい。

【0022】図6は、紛失した携帯端末の所有者から、例えばブッシュホン（電話機）によって非常時連絡先電話番号をダイヤルし、セキュリティコントローラ10に情報保護を要求した場合の保護システムの動作手順を示す。ここでは、上記情報保護の要求を受け付けた時点で、紛失携帯端末がPHSシステムと通信可能な状態にあり、セキュリティコントローラ10が紛失携帯端末のアクセスに成功した場合の動作例を示す。また、図6における動作S1:134～S5:138、および後述する図7における動作S6:158～S7:159を実行するセキュリティコントローラ10の動作フローチャートを図10に示し、以下図10の動作ステップも参照して動作説明する。

【0023】携帯端末の紛失に気付いた所有者が、電話機18で非常時連絡先の電話番号をダイヤルすると（動作U1:131）、セキュリティコントローラ10との間にコネクションが確立する。この場合、発呼時に電話機から発信される呼制御信号が保護要求121となる。セキュリティコントローラ10側では、上記非常時電話番号への着信は、音声応答システムに接続され、最初の自動応答メッセージ（認証確認メッセージ）122として、例えば、「登録者IDと#、それに引き続いてパスワードと#を押してください」という内容の音声メッセージを出力する（動作S1:134、図10のステップ101～205）。所有者は、上記音声メッセージに答えて、数字キーと#ボタンを用いて、登録者IDとパスワードを入力する（動作U2:132）。これらの入力データは、認証データ123として送信される。

【0024】セキュリティコントローラ10は、上記認証データ123を受信すると、登録者IDと同一のIDをもつ登録済のセキュリティ管理データレコードを検索し、受信したパスワードが登録済の認証情報84と一致するか否かを判定し、情報保護の要求者が登録された人物である事を確認した後、要求確認メッセージ124を出力する（動作S2:135、図10のステップ206～208）。上記要求確認メッセージ124は、例えば、「只今から情報保護動作を開始します。携帯端末が発見できなかった場合、引き続いて、探索動作を続けます。すぐに見つからない場合は、後日、連絡します。連絡先の電話番号と#ボタンを押して、しばらくお待ちください。」のような内容とする。

【0025】所有者が、電話番号入力と#ボタン操作（動作U3:133）行くと、セキュリティコントローラは、PHSシステムDB11に対して、セキュリティ管理データレコードで登録されているPHS電話番号を

指定して、携帯端末検索要求127を送信する(動作S3:136、図10のステップ209~211)。PHSシステムDB11は、上記検索要求(127)を受信すると、データベースから該当するPHS電話番号を持つ携帯端末が位置登録されているかを検索し、その結果を携帯端末検索レスポンス128として、セキュリティコントローラ10に送信する(動作N1:139)。

【0026】セキュリティコントローラ10は、目的携帯端末が位置登録されている場合、その携帯端末に、予め登録してあった処理番号85で情報保護の種類を指定した形で、情報保護命令129を送信する(動作S4:137、図10のステップ212~214)。上記情報保護命令129を受信した携帯端末14は、情報保護プログラムを実行し、これが完了すると、必要に応じて保護データを伴う保護終了報告130をセキュリティコントローラ10に送信する(動作P1:140)。

【0027】セキュリティコントローラ10は、上記保護終了報告130を受信すると、退避すべき保護データがなければ直接、もしあれば、これを上記セキュリティ管理データレコードと対応付けて蓄積(退避データ記録)した後、情報保護の終了通知126を回答(動作S5:138、図10のステップ215~208)し、手続きを終了する。上記情報保護の終了通知126は、例えば、「携帯端末の情報の保護を完了しました。」の内容をもつ音声メッセージであり、保護データを回収した場合は、その旨を示す音声メッセージを追加する。

【0028】尚、上記実施例において、PHSシステムDBに対する携帯端末検索要求動作S3とその応答動作N1は、上記携帯端末検索要求127に回答して、PHSシステムDBが、目的携帯端末が位置登録されている基地局を見つけ出し、この基地局の識別子と対応関係にある基地局所在地(住所)情報を検索し、例えば、上記基地局所在地を中心としたセル半径をもって目的携帯端末の概略的な現在位置を表し、これを上記携帯端末検索レスポンス128によってセキュリティコントローラに通知し、セキュリティコントローラが、上記現在位置情報を検索要求者に通知する場合に有効となる。また、図8で説明するように、携帯端末の所有者が情報保護を要求した時点で携帯端末が通信不能の状態にあった場合に、この端末が無線ネットワークに位置登録したのを検出して、自動的に情報保護命令を発行する場合に有効となる。

【0029】もし、このような端末所有者への端末位置情報サービスを全く必要としない場合は、PHSシステムDBへの端末検索要求127を省略し、目的携帯端末が位置登録されているか否かに無関係に、セキュリティコントローラ10が、上記動作S3において目的端末への呼(コネクション)設定を試み、コネクションが設定された場合に動作S4を実行するようにしてもよい。目的端末が通信不能の状態にあった場合は、セキュリティ

コントローラ10が、所定の繰返しパターンで自動的に発呼を繰返すようにすればよい。

【0030】図7は、図6で示した情報保護の要求を受け付けた時点で、紛失携帯端末を発見できなかった場合の動作例を示す。図7の動作シーケンスで、PHSシステムDB11がセキュリティコントローラ10に携帯端末検索レスポンス128を送信するまでの手順は図6と同様である。この場合、セキュリティコントローラ10から検索要求のあった携帯端末の現在位置確認に失敗した場合、PHSシステムDB11側で、上記携帯端末の情報レコードに、セキュリティコントローラ10で探索中の端末である旨を示すフラグをたてておくといふ。この例では、セキュリティコントローラ10は、PHSシステムDB11から位置確認失敗を示す携帯端末検索レスポンス128を受信し、動作S4:137において、所有者に、例えば、「お捜しの携帯端末が見つかりません。引き続いて端末の監視を行います。ここで端末捜査と情報保護を打ち切る場合は2#を、継続する場合1#を押してください。」の内容をもつ音声メッセージ(常駐確認メッセージ)151を送信する(図10のステップ219)。

【0031】所有者が「2#」を選択した場合は、セキュリティコントローラ10は、「これでサービスを終了させていただきます。」の音声メッセージを出力して(動作S6:158、図10のステップ220、221、227)、通信を終了する。所有者が「1#」を選択した場合は、上記動作S6:158で、例えば、「お客様の連絡先電話番号は、XXXXXXXXXXで間違いありません。宜しければ1#、電話番号を変更する場合は2#を押し、再度、電話番号を入力した後、#を押してください。」の内容の音声メッセージ(連絡先確認メッセージ)153を送信する(図10のステップ221、222)。所有者が、上記確認メッセージに回答操作(動作U6:157)すると、セキュリティコントローラは、上記回答操作による連絡先レスポンス154の内容を解析し、「1#」の場合は、例えば、「これでサービスを終了させていただきます。」の内容をもつ終了メッセージ155を送信した後、通信を終了する。もし、上記確認メッセージに回答して「2#」と電話番号が入力された場合は、再度、電話番号確認メッセージを送信した後、同様の動作を繰り返す(動作S7:159、図10のステップ223~227)。

図8は、紛失した携帯端末を自動的に見つけ出すための常駐保護処理の動作手順を示す。また、図11に、上記図8中の動作S8:166とS9:167と対応するセキュリティコントローラ10の動作フローチャートを示し、以下図11も参照して動作説明する。紛失した携帯端末14の電源がONになると、内蔵PHS電話機能によって、基地局に位置登録要求161が発信され、PHSシステムDB11が端末の位置登録(動作:168)

を行う。PHSシステムDB11は、何れかの基地局から位置登録情報161を受信すると、位置登録の動作過程で、上記携帯端末の情報レコード中に、セキュリティコントローラ10で探索中の端末である旨を示すフラグを見つけ、セキュリティコントローラ10に対して、紛失端末位置を示す位置登録通知162を送信する。

【0032】セキュリティコントローラ10は、PHSシステムDBからの位置登録通知の受信待ち状態(図11のステップ101)にあり、上記位置登録通知162を受信すると、紛失携帯端末14に対して、PHS電話システムによる通信を開始し、情報保護命令129を送信する(動作S8:166、図11のステップ243~245)。携帯端末14は、上記情報保護命令129に応答して、図6で示したのと同様に情報保護プログラムを実行し、保護終了報告130をセキュリティコントローラ10に送信する。セキュリティコントローラ10は、上記保護終了報告130を受信すると、動作S9:167において、もし、保護データがあればこれを蓄積(避難データ記録し(図11のステップ246~248)、セキュリティ管理データレコードに情報保護終了を記録した後、上記データレコードに記憶してある端末所有者の連絡先に自動的ダイヤルし、情報保護の報告165を音声メッセージで通知する(図11のステップ249~251)。上記実施例では、保護要求のあった携帯端末が位置登録をした時点で、PHSシステムDB14が、情報保護要求の有無をチェックし、自動的にセキュリティコントローラに通知する方式となっているが、PHSシステムDB14にこのような特殊な機能を付加したくない場合は、セキュリティコントローラ10が、定期的に携帯端末に発呼を繰り返すことによって、動作S8:166の切っ掛けを得るようにすればよい。

【0033】図9は、上述した情報保護動作の実行時に携帯端末、セキュリティコントローラ、PHSシステムデータベース間で通信するメッセージ70のフォーマットの一例を示す。メッセージフォーマット70の基本構造は、図3に示したものと同様で、データ内容74がメッセージ種類によって異なっている。301は、図6及び図7で示した携帯端末検索要求メッセージ127のデータ内容を示す。処理命令メッセージ305と携帯端末電話番号79の2つのフィールドからなり、上記処理命令メッセージ305には、PHSシステムDB11に対する要求内容を示す文字列が設定され、携帯端末電話番号79には、検索対象となる携帯端末のPHS電話番号が設定される。

【0034】302は、図6及び図7で示した携帯端末検索レスポンス128と、図8で示した位置登録通知162に用いるメッセージのデータ内容74を示す。データ内容は、携帯端末の有無310、携帯端末電話番号82、位置情報306の3つのフィールドからなり、携帯端末電話番号82には、検索対象となった携帯端末のP

HS電話番号が設定され、位置情報306には、上記携帯端末が位置するPHSシステム内の接続ポイント(基地局)を示す位置情報が設定され、この位置情報によって、携帯端末の概略的な現在位置を知ることができる。

【0035】303は、図6および図8で示した情報保護命令129のメッセージにおけるデータ内容74を示し、携帯端末識別ID81、携帯端末電話番号82、登録者ID83、認証情報84、処理命令311および暗号鍵C:307を含む。携帯端末識別ID81、携帯端末電話番号82、登録者ID83、認証情報84、処理番号85は、セキュリティ管理データとして登録されたものであり、情報保護命令129を受信した時、携帯端末14側で、受信メッセージの信頼性をチェックするために利用される。暗号鍵C307は、公開暗号鍵方式の公開暗号鍵であり、携帯端末は、この暗号鍵Cを用いてセキュリティコントローラに送信する保護情報を暗号化する。

【0036】304は、図6及び図8に示した保護終了報告130のメッセージにおけるデータ内容74を示し、メッセージ種別ID308とデータ309の2つのフィールドからなる。メッセージ種別ID308は、これに続くデータフィールド309に、例えば、保護終了報告コードのみを含む場合は「0」、保護終了報告コードと保護データとを含み上記保護データに続きがない場合には「1」、保護データに続きデータがある場合は「2」が設定される。データフィールド309に内容は、暗号鍵C307を用いて暗号化されている。

【0037】図12は、図6、図7、図8における動作N1:139、N2:168を実行するPHSシステムDBの動作フローチャートを示す。PHSシステムDB11は、受信メッセージをチェックし(ステップ261)、受信メッセージが携帯端末からの位置登録要求であれば、動作N2:168を実行する。この場合、通常の位置登録動作を行い(ステップ271)、もし、その携帯端末についてセキュリティコントローラから探索要求がなされいることが判明すると、セキュリティコントローラ宛の通知情報(図8の位置通知162)を作成し(272)、セキュリティコントローラへ送信(273)した後、メッセージ受信待ち状態に戻る。

【0038】セキュリティコントローラから携帯端末検索要求127を受信した場合は、動作N1:139を実行する。この場合、先ず、携帯端末検索要求を解析し(264)、検索要求で指定されている携帯端末電話番号(図9に示されている携帯端末電話番号79)に基づいてデータベース情報を検索し(265)、目的端末が位置登録されているか否かをチェックする(266)。目的端末が位置登録されていた場合は、図9に示したデータ内容フォーマット302におけるフィールド310に携帯端末有りを示す「1」、フィールド82に目的携帯端末の電話番号、フィールド306に上記目的携帯端

末を收容している基地局情報が設定された応答メッセージ128を作成し(267)、セキュリティコントローラに送信する(270)。目的携帯端末の位置が未登録の場合、上記フィールド310と306の「0」が設定された応答メッセージ128を作成し(268)、これをセキュリティコントローラに送信する(270)。

【0039】図13は、本発明が適用される携帯端末におけるデータ保護動作Pの詳細を示す1フローチャートである。携帯端末は、通常のデータ処理動作状態282において通信制御部から割り込みを受けた場合(281)、携帯端末のROMに格納されているデータ保護に専用ソフトウェアを起動し、通信メッセージを解析する(284)。PHS電話機能および通信制御部が受信待ち状態にあり、CPU本体部の電源が未投入状態にある場合は、CPU電源を自動的に投入した後、上記通信メッセージの解析を行う。

【0040】上記割り込み原因となった通信制御部での受信メッセージがセキュリティコントローラからの情報保護命令129であれば、図3で説明したように、データ部が暗号鍵B:86で暗号化されているため、その場合は、暗号鍵Bに対応して予めROMに記憶されている秘密鍵を用いてメッセージ内容を解読する。上記通信内容が情報保護命令129でなければ(284)、通常の通信処理(282)を行い、情報保護命令の場合は、認証チェックを行う(286)。認証チェックは、上記情報保護命令中に含まれる認証情報(図9におけるフィールド85の内容)と、携帯端末情報保護の登録時に携帯端末内に記憶しておいた正当な所有者の認証情報(パスワード)とを比較することによって行う。認証結果に問題があれば以降の処理を省略して最初のステップ281へ戻る。

【0041】認証に問題がなければ、保護命令の内容を解析し(287)、処理番号フィールド85の値からデータ転送の可否を判定し(288)、データ転送の必要がなければステップ291へ進む。データ転送の必要があれば、情報保護命令中の暗号鍵(暗号鍵C:307)を用いて端末情報(保護データ)を暗号化し(289)、暗号化された端末情報をセキュリティコントローラへ送信(290)した後、ステップ291に進む。ステップ291では、端末情報の機密保護(無効化または書き換え)処理を行う(291)。データ機密保護は、例えば、端末情報のメモリ消去、または偽データへの交換によって達成する。データ機密保護が終了すると、データ保護終了メッセージをセキュリティコントローラへ送信し(292)、割り込み処理を終了し、元の状態に戻る。

【0042】図14は、セキュリティコントローラ10の構成を示す。セキュリティコントローラ10は、CPU20、ROM21、RAM22、データファイル23、通信制御部24、PHSシステムDBとの通信イン

タフェース25、携帯端末との通信インタフェース26、音声応答機能をもつ音声制御部27、電話インタフェース28、および内部バス29からなる。CPU20は、ROM21に用意された制御プログラムに従って、通信制御部24および音声制御部27を制御し、通信インタフェース25を介してPHSシステムDBと、通信インタフェース26を介して携帯情報端末と、電話インタフェース28を介して電話機と通信する。RAM22は、プログラムのワークエリアとして利用され、PHSシステムDBあるいは携帯端末所有者からのデータの一時保存に利用される。ファイル装置23は、セキュリティ管理データレコード、紛失端末からの回収データ、あるいは常駐による保護処理動作に必要な情報等の保存に利用される。

【0043】図15は、携帯端末14の構成を示すブロック図である。本発明を適用する携帯端末14は、CPU31、ROM32、RAM33Aおよび33B、補助記憶装置34、表示装置(例えば、液晶ディスプレイ)35、入力装置36、電源制御部37、通信インタフェース38、通信制御部39、バス40、電源制御線41、通信割り込み制御線42からなる。CPU31は、バス40を介して、ROM32、RAM33A、33B、補助記憶装置34、表示装置35、入力装置36、通信インタフェース38との間でデータを送受信する。また、電源制御部37は、電源制御線41を介して、上記各要素の電源オン、オフを制御する。通信制御部39は、本実施例では、PHS無線通信を実現するための機能として、例えば、アンテナ、高周波回路、PHSの通信手順制御および通信内容チェック手段を備え、通常のPHS通信では、通信インタフェース38を介してCPU31と通信メッセージデータのやり取りを行い、通信割り込み制御信号を発生して、CPU31または電源制御部37に割り込みをかける。

【0044】ROM32は、携帯端末としての機能を実現するための各種のソフトウェアと、本発明による端末情報保護を実施するための専用ソフトウェア及び制御情報が格納される。RAM33Aおよび33Bは、電源でバックアップされており、RAM33Aは、情報保護を必要としない通常のデータ格納用として、また、RAM33Bは、本発明を適用して保護すべき特定ファイルデータの格納用として用いられる。上記携帯端末のCPUは、通信制御部からの割り込みを受けると、ROM32に用意された専用ソフトウェアを実行し、上記割り込みが端末情報保護命令の受信によるものであれば、RAM33B内の蓄積情報を保護対象として、前述のデータ回収および保護処理を実行する。

【0045】上記実施例では、各端末で保護対象となる情報を特定のメモリに蓄積しておき、端末紛失時に上記特定メモリ内の全情報に対して情報保護動作がかかるようにしたが、情報保護はデータファイル名を特定して行

うようにしてもよい。例えば、各携帯端末において、保護対象となる情報を特定のファイル名、または特定の頭文字をもつファイル名で管理しておき、情報保護の登録要求時に、端末所有者が保護対象とすべきファイル名

(または頭文字等のファイル識別情報)を指定して、これを上記専用ソフトウェアが記憶しておき、情報保護命令が発生した時、上記特定ファイル名のファイルに対して保護処理を実行するようにしてもよい。

【0046】また、実施例では、端末所有者が電話機を介してセキュリティコントローラと直接交信し、セキュリティコントローラ側が音声応答機能によって情報保護要求を受付制御するようにしたが、紛失端末の所有者がテキストデータの送受信機能を備えた他の無線端末、またはネットワーク5に接続された他の端末からセキュリティコントローラにアクセスし、端末情報保護に必要な情報をデータメッセージ形式で交信するようにしてもよい。また、紛失端末の所有者が普通の電話機で通報した情報保護要求をセキュリティシステム側で係員が受付け、端末所有者が指定した登録者IDに基づいて係員が専用端末からセキュリティコントローラにアクセスし、所有者の認証に必要なパスワード等のデータを係員端末から入力することによって、情報保護を実行するようにしてもよい。

【0047】

【発明の効果】以上の説明から明らかなように、本発明によれば、携帯端末の通常の使用時ににおいて、ファイルアクセス権限確認のためのパスワード入力等の面倒な操作を強制することなく、携帯端末紛失時に端末情報の保護あるいは情報回収が可能となる。また、情報保護要求時に、無線ネットワークにおける端末位置登録機能を利用すれば、紛失端末の概略的な現在位置を知ることができるため、この位置情報に基づいて紛失端末の回収にも役立つことができる。

【図面の簡単な説明】

【図1】本発明による携帯端末情報保護を実現するネットワークシステムの構成図。

【図2】端末情報保護の登録手順の1実施例を示す図。

【図3】上記端末情報保護の登録時に携帯端末とセキュリティコントローラとの間で通信されるメッセージフォーマットの1実施例を示す図。

【図4】上記端末情報保護の登録時に携帯端末に表示される画面の1実施例を示す図。

【図5】上記端末情報保護の登録時にセキュリティコントローラが実行する制御プログラムの処理手順の1実施例を示すフローチャート。

【図6】端末紛失時に実行されるネットワークで実行される情報保護手順の1例を示すシーケンス図。

【図7】端末紛失時に実行されるネットワークで実行される情報保護手順の他の例を示すシーケンス図。

【図8】端末紛失時に実行されるネットワークで実行される情報保護手順のさらに他の例を示すシーケンス図。

【図9】情報保護時に通信されるメッセージフォーマットの1実施例を示す図。

【図10】情報保護時にセキュリティコントローラが実行する制御プログラムの1実施例を示すフローチャート。

【図11】情報保護時にセキュリティコントローラが実行する制御プログラムの他の実施例を示すフローチャート。

【図12】情報保護時にPHSデータベースシステムが実行する制御プログラムの1実施例を示すフローチャート。

【図13】情報保護時に携帯端末が実行する制御プログラムの1実施例を示すフローチャート。

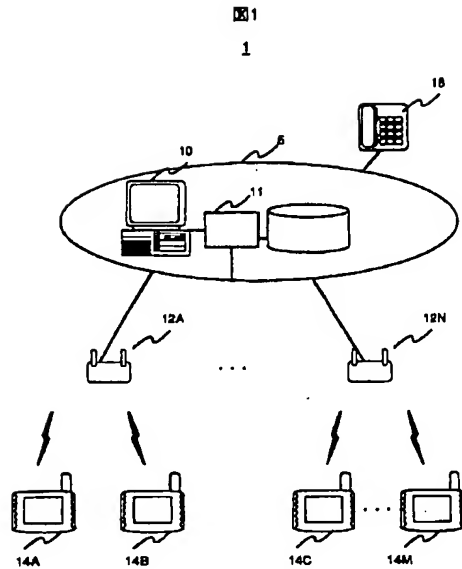
【図14】セキュリティコントローラの構成の1例を示すブロック図。

【図15】携帯端末の構成の1例を示すブロック図。

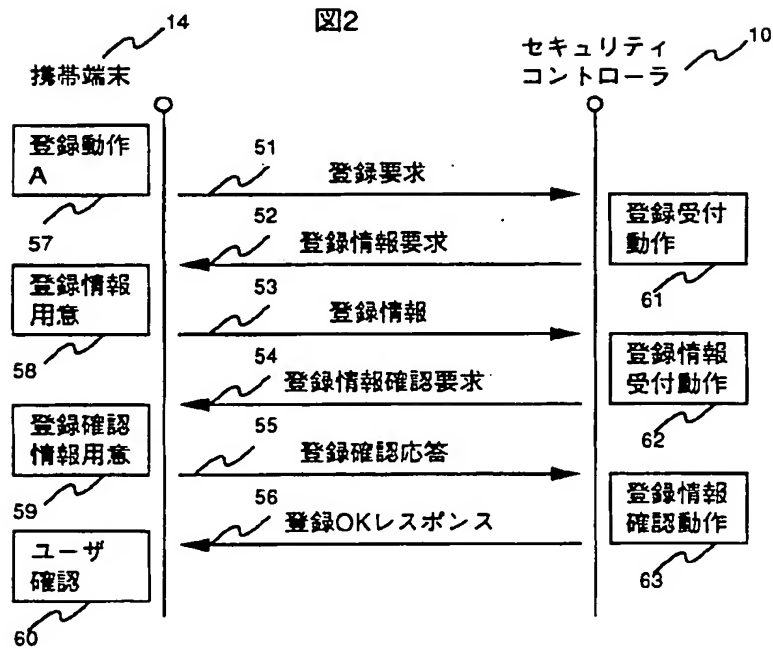
【符号の説明】

1…無線ネットワークシステム、5…有線網、10…セキュリティコントローラ、11…PHSシステムデータベース、12…基地局、14…携帯端末、18…電話、51…登録要求、52…登録情報要求、53…登録情報、54…登録情報確認、55…登録確認応答、56…登録OKレスポンス、70…通信メッセージフォーマット、71…識別ID、72…動作ID、73…データ量、74…データ内容、75…CRC、76…登録要求データ、77…登録情報データ、78…登録OKレスポンスデータ、90…登録開始画面、91…登録入力画面、92…所有者確認画面、121…保護要求、122…認証確認メッセージ、123…認証データ、124…要求確認メッセージ、125…要求送付、126…終了通知、127…携帯端末検索要求、128…携帯端末検索レスポンス、129…情報保護命令、130…保護終了報告及び保護データ、151…常駐確認メッセージ、152…常駐レスポンス、153…連絡先確認メッセージ、154…連絡先レスポンス、155…終了メッセージ、301…携帯端末検索データ、302…携帯端末検索レスポンスデータ、303…情報保護命令データ、304…保護データ。

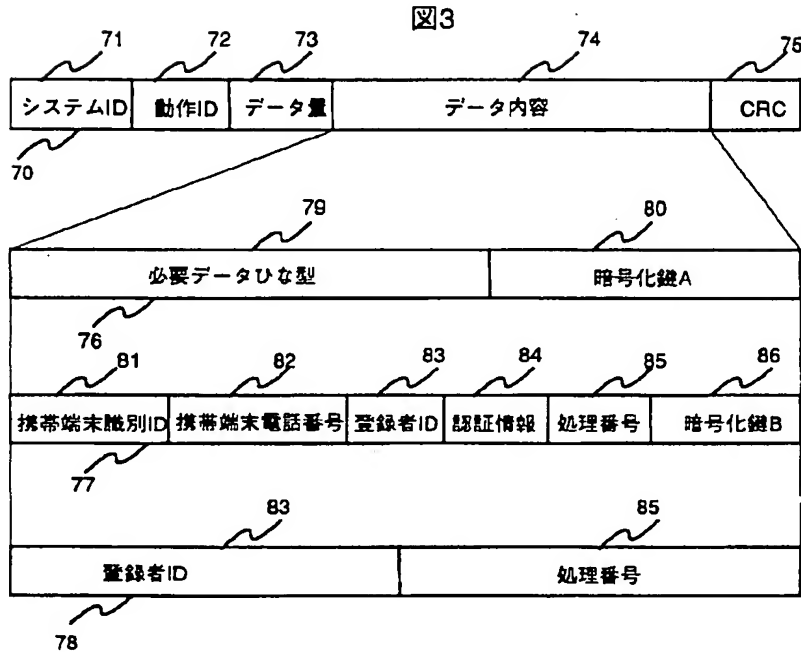
【図1】



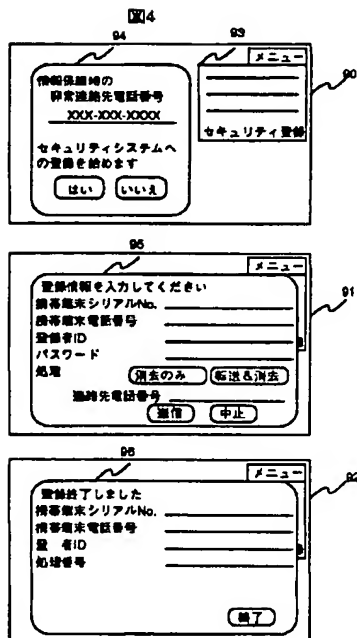
【図2】



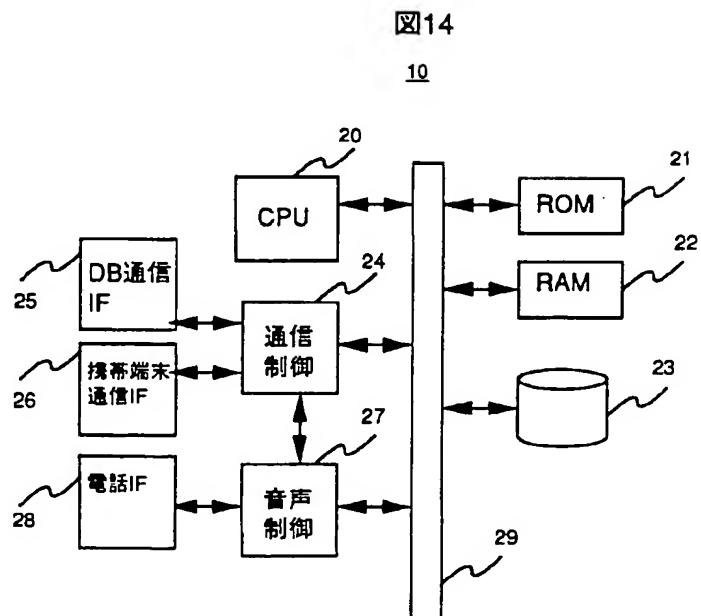
【図3】



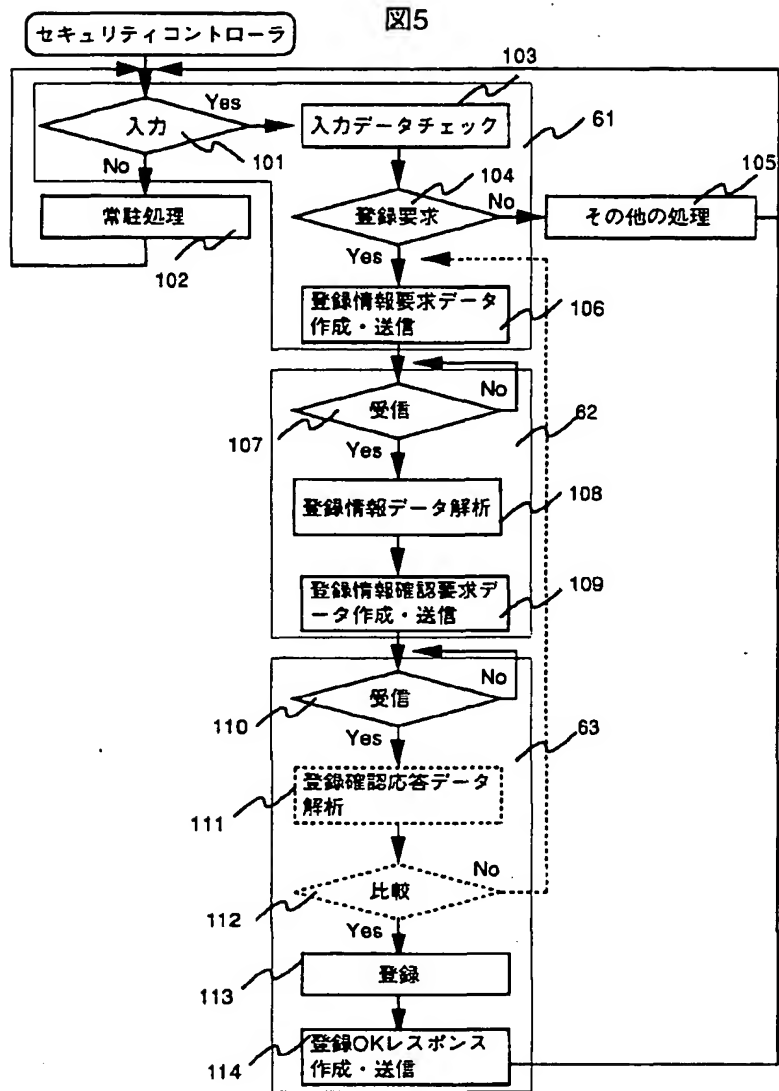
【図4】



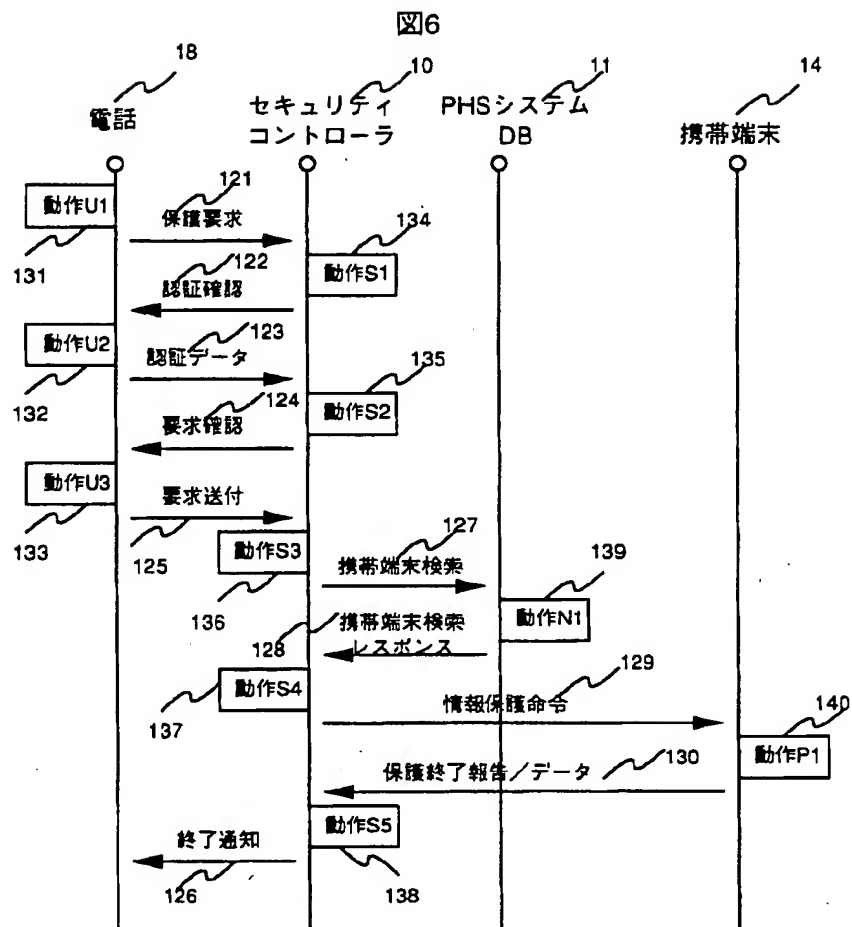
【図14】



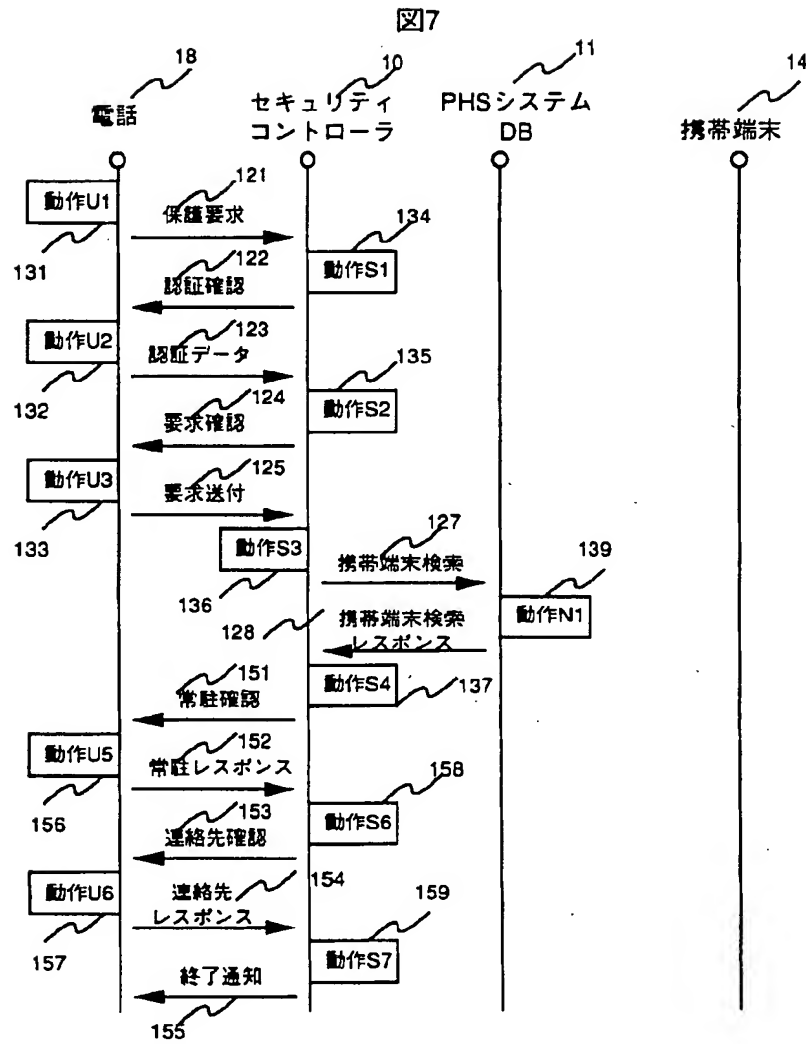
【図5】



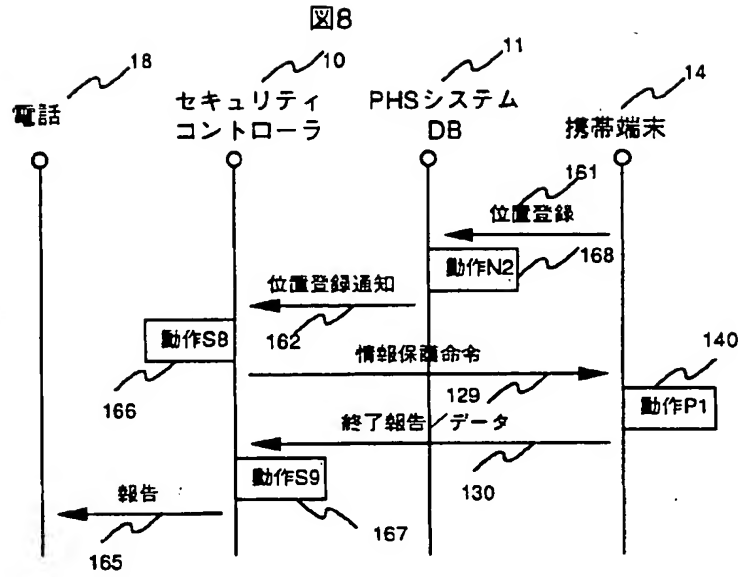
【図6】



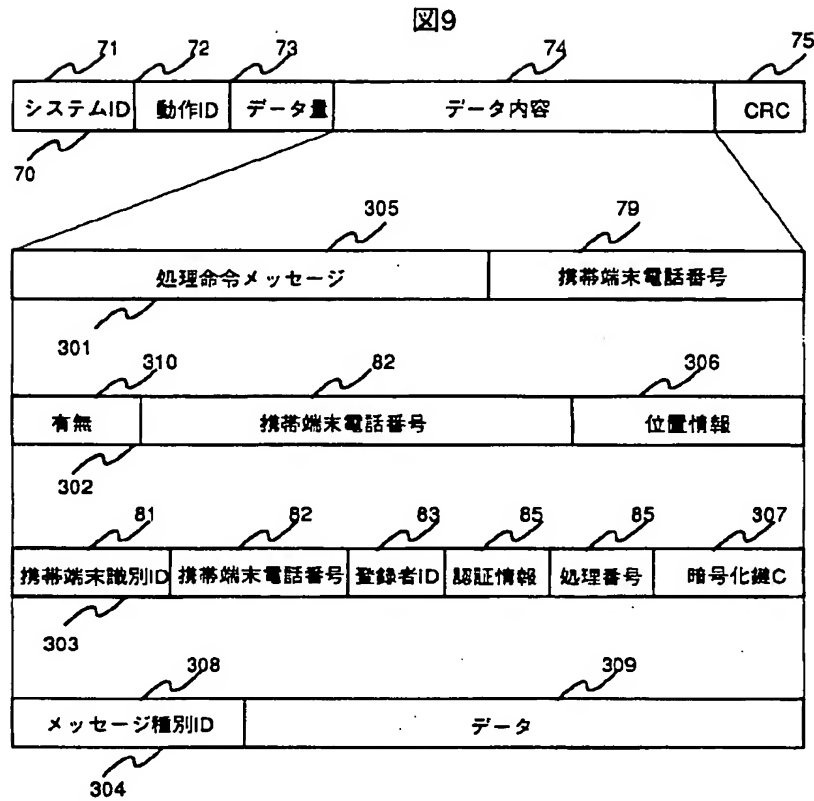
【図7】



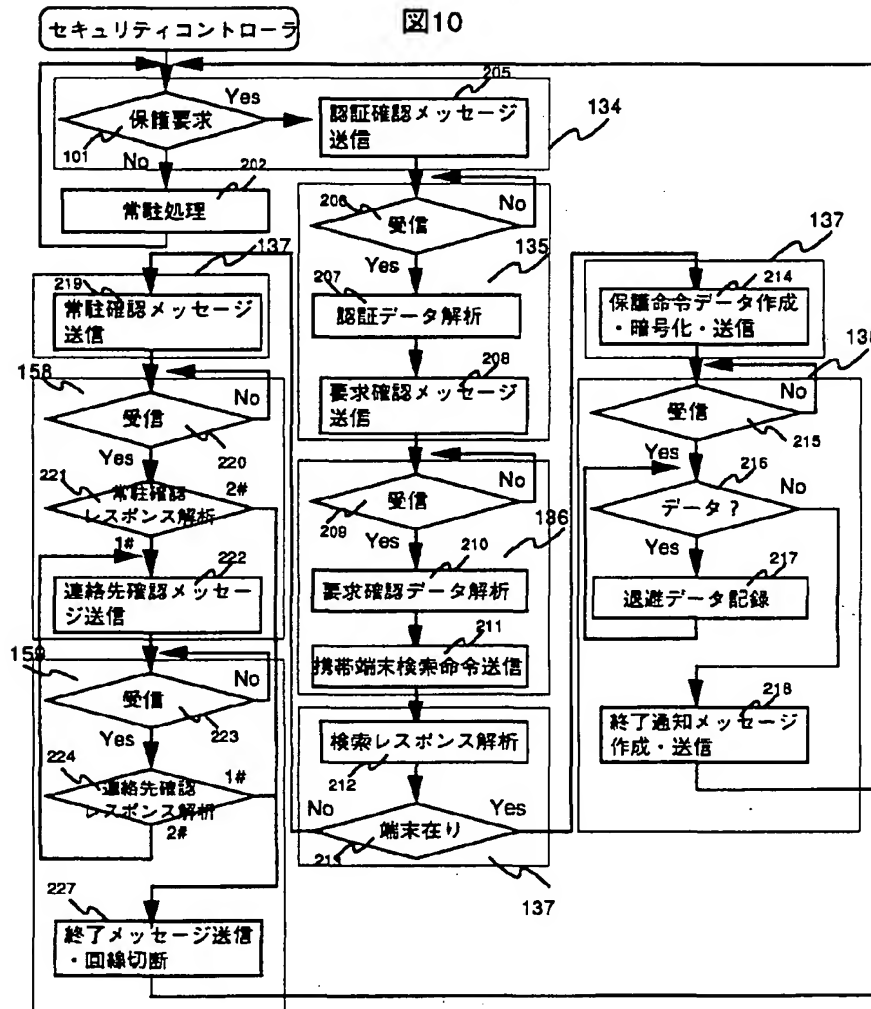
【図8】



【図9】

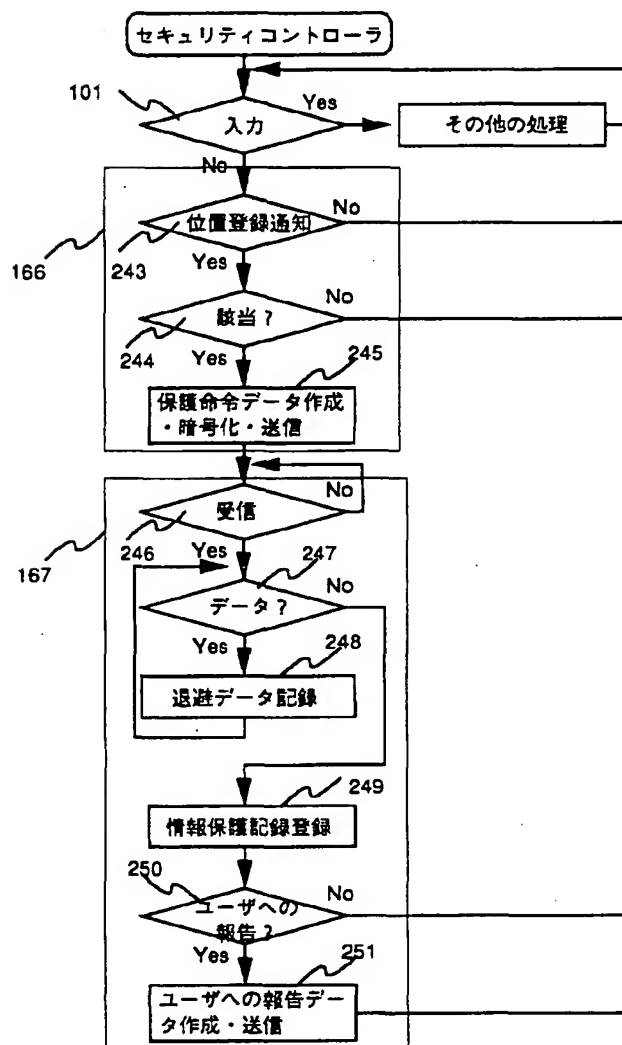


【図10】

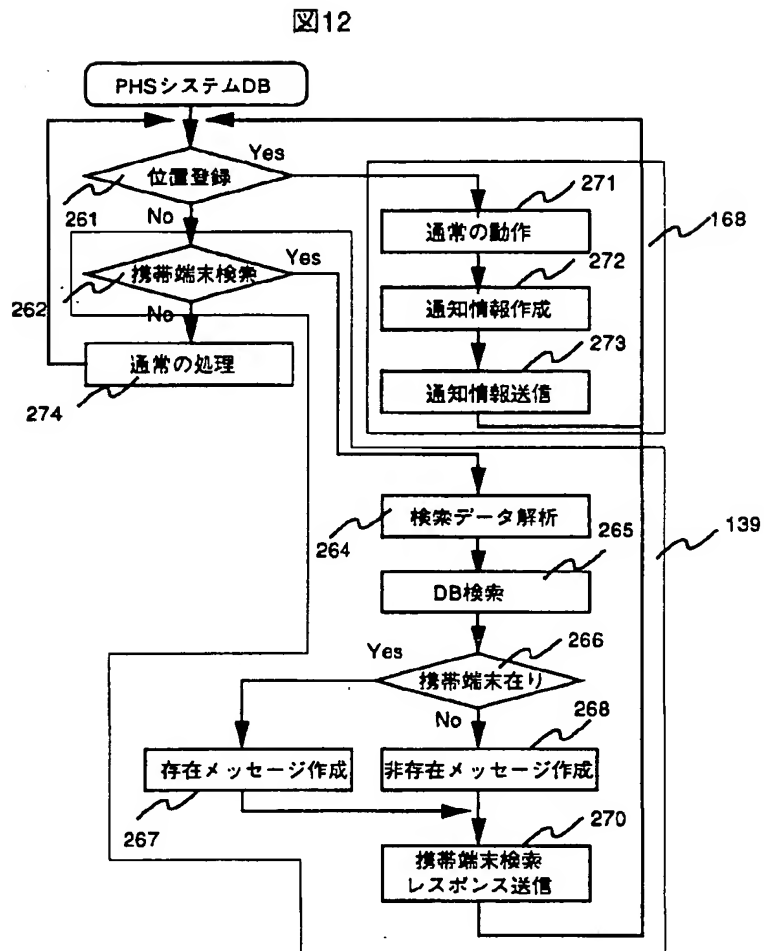


【図11】

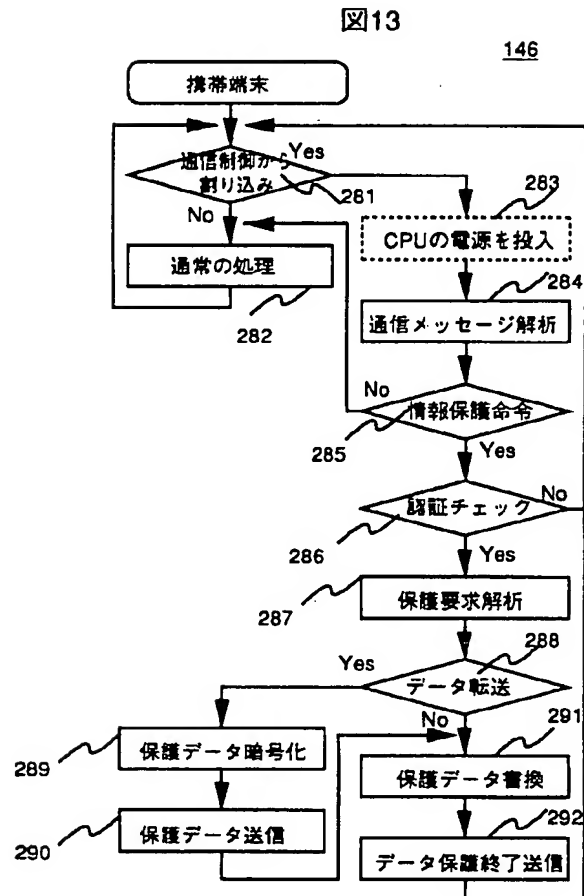
図11



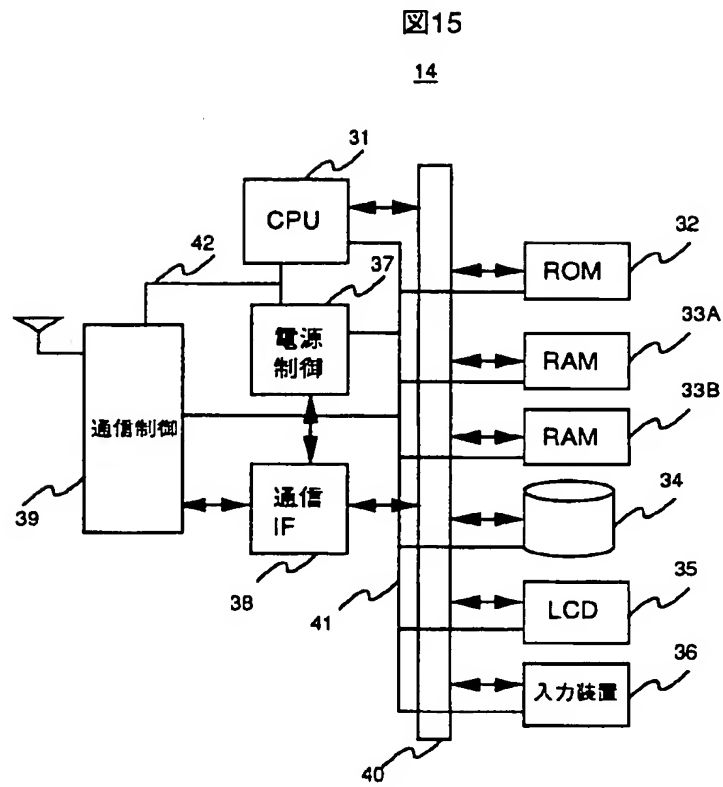
【図12】



【図13】



【図15】



フロントページの続き

(51)Int.Cl.⁶

H04M 11/00

識別記号

302

庁内整理番号

FI

H04L 9/00

H04Q 7/04

技術表示箇所

673A

D